Cryptographic Schema for IoT End-devices

Azize Karagoz[1], Busra Calmaz[2], Didem Genc[3], and Serap Sahin[4]

[1,2,3,4,5]Computer Engineering, Izmir Institute of Technology

***Abstract*—IoT notion began to play an important role in human life. We are trying to make the things accessible through the internet by connecting them to network in order to interact with each other. However this brings important security concerns with it. IoT comprises of interaction of many devices, people, services etc. Things called as end-devices generally have limited power, low computation capability and restricted memory. Therefore, ensuring security for such a resource-limited device is a great challenge since conventional cryptographic algorithms require heavy computational power and large memory. In order to handle these limitations lightweight cryptographic algorithms are used. In this paper, by considering limitations of end-devices, we proposed a cryptographic schema, which uses lightweight cryptographic algorithms, targeting to ensure security in network layer. We aimed to address the secrecy, integrity and authentication concerns by using PRESENT and Diffie-Helman Key Exchange, SHA-256, and Hummingbird-v2 algorithms respectively.**

I. INTRODUCTION

It is undeniable fact that IoT greatly facilitates human life. For this reason, it has been adopted in many areas. It is possible to encounter IoT enabled devices everywhere. As an example; it is really nice that the air conditioner learns the preferred ambient temperature that the household always use, and adjusts the temperature to that degree before they come. To do this, air conditioner may communicate with the smart car to verify that one of the household member is on the road to home. As this simple scenario indicates, IoT notion involves many-to-many type of interaction like the communication between the smart car and air-conditioner.

According to Gartner there will be 5.8 billion IoT devices connected to the internet in 2020. Predictably it is nearly impossible to estimate all interactions between these devices priorly. So, the security gains great importance. Unauthorized access to data, monitoring and changing integrity of message or misuse of data can led to significant faults in IoT systems.

IoT environment consists of heterogeneous hardware devices which are divided into two types; high-end devices and low-end devices. High-end devices have sufficient resource to run the conventional cryptographic algorithms. However, low-end devices are resource-constraint. They have less than 10kB of RAM and less than 100kB of flash memory. Therefore, ensuring security by using conventional cryptographic algorithms such as; AES, ECC, RSA etc. can not be possible. Lightweight cryptographic algorithms, which require low computational power and minimum memory, are used to ensure security of low-end IoT devices.

In general, IoT architecture consists of 3 layers: perception layer, network layer and application layer. Perception layer collects data from surrounding environment through heterogeneous type of sensors. Acquired data from perception layer is conveyed to network layer for reliable data transmission. Application layer is responsible for performing massive data processing and statistical analysis by making use of cloud technologies.

Firstly it is crucial to investigate the domain to develop a cryptographic schema for IoT end devices. For this reason, the IoT attacks classified by layers are reviewed. Perception layer challenges are generally Unauthorized Access to Tags, Node Capture Attacks, Tag Cloning, False Data Injection Attacks. Attacks on the network layer are similar to those on traditional networks. The network layer challenges are Spoofing Attack, Sinkhole Attack, Sleep Deprivation Attack, Denial of Service (DoS) Attack, Unsecured Protocols. Lastly, application layer security challenges are Phishing Attack, Malicious Virus/worm, Sniffing Attack, Malicious Scripts[1].

In this study, we aim to make communication secure between the sensor node and gateway, which are in the same local network. Therefore, we proposed a cryptographic schema that addressing confidentiality and identification for network layer of IoT low-end devices. We used a lightweight cryptographic algorithm PRESENT for message encryption. We made used of Diffie-Helman Key Exchange algorithm for key sharing. Also a nonce value is used for identification. The rest of the paper is organized as follows. Section II gives the background information of our work by explaining used cryptographic algorithms separately. Section III presents the design and implementation details. In Section IV, related work is given. Lastly, in Section V we conclude our paper and give the future work.

II. BACKGROUND INFORMATION

In this part of the paper, cryptographic algorithms, which are used in the implementation, are explained in briefly.

A. PRESENT

The block cipher PRESENT consists of substitution permutation network with 64 bits block size. It operates 31 rounds and supports two key lengths of 80 and 128 bits. A round is a combination of ByteSub, ShiftRow, MixColum and AddRoundKey operations. The compact size of Present algorithm much more smaller than the AES[2]. Encryption procedure consists of 3 steps:

In the first part, the data and the key go through the xor process. The last 64 bit data is taken and this 64 bit data is

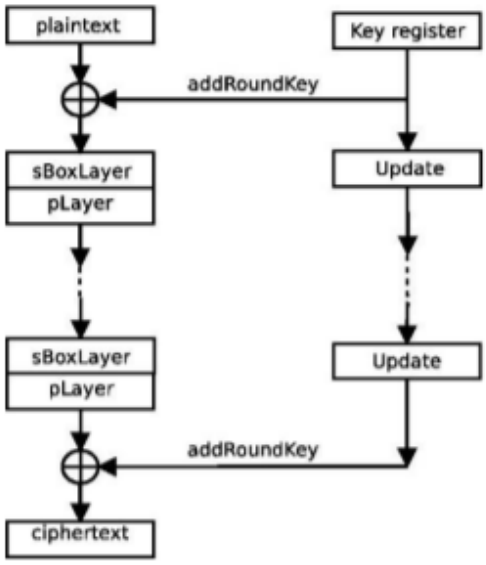

Fig. 1. PRESENT algorithm round[2]

divided into 16 blocks each containing 16 bits for the next process.

Byte substitution layer (sboxLayer): In these layer a nonlinear substitution block is applied to each 16 block, that obtained previous step, are passed through the substitution boxes and each value in these boxes is replaced by the values in the substitution blocks. The hexadecimal notation of S-box is given in Figure 2.

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Fig. 2. S-box from PRESENT algorithm[2]

Bit Permutation (pLayer): In this layer, each bit of 64 bit input is mixed by bit to bit substitution.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Fig. 3. Substitution table of the PRESENT algorithm[2]

Key expansion function: addRoundKey: After these operations, the key is updated to use for next round. The key is updated as follows:

$$b_j -> b_j \oplus x_i$$

where round key $k_i = k_{63}....k_0$ for 1 < i < 32 and present state $b_{63}....b_0$, addRoundKey consists of the operation for 0 ≤ j ≤ 63 [1]. During the encryption procedure, these steps are repeated 32 times and encrypted data is transmitted.

B. Diffie-Helman Key Exchange Algorithm

Diffie Hellman key exchange algorithm was developed by Whitfield Diffie and Martin Hellman in 1976 [3]. It provides securely exchanging cryptographic keys over a public communication channel. The algorithm based on derivation of keys by the communicator's itself instead of changing the keys. For example, Alice and Bob communicate with each other by using symmetric cipher. In this algorithm, Alice and Bob do not actually exchange keys, they derive the key jointly. The steps of the Diffie Hellman key exchange algorithm is given below.

- Bob and Alice agree between them on a large prime p and generator(base) g (0< $g < p$).
- Alice chooses her private key **a** and calculates g^a **mod p** (her public key). Then Alice sends her public key to Bob.
- Bob also chooses his private key **b** and calculates g^b **mod p** (his public key). Then Bob sends his public key to Alice.
- They calculate $g^(a.b)$ **mod p** and know a shared secret between them.

Diffie and Hellman take advantage of the difficulty of the discrete logarithm problem. An attacker who listens to Bob or Alice knows p,g, and public key of Alice and Bob. But it is hard to calculate their private key (if p is a large prime number) because of the discrete logarithm problem.

$$x = g^a mod p -> Easy problem$$

$$a = log_g x -> Hard problem$$

III. DESIGN AND CONTRIBUTION

A well known cryptographic algorithm schemes includes different security protocols such as TableIII[4]. In our study, we proposed a cryptographic scheme which includes confidentiality, integrity and availability, also known as the CIA triad[5].

TABLE I
A SUITE OF CRYPTOGRAPHIC ALGORITHMS

Algorithm	Purpose
Advanced encryption standard (AES)	Confidentiality
Rivest shamir adelman (RSA)/ Elliptic curve cryptography (ECC)	Digital signatures key transport
Diffie-hellman (DH)	Key agreement
SHA-1/SHA-256	Integrity

Normally the advanced encryption standard AES used to ensure confidentiality for security communication. AES is not appropriate the limited end device. So in our project

we uses lightweight symmetric encryption algorithm which called PRESENT. The asymmetric algorithm is used to digital signatures and key transport. Usually the Rivest shamir adelman (RSA) and the diffie-hellman (DH) asymmetric key agreement algorithm is used to key agreement. In our project we use diffie-hellman (DH) asymmetric key agreement algorithm to provide authorization and identification IoT device . The secure hash algorithm used for provide integrity of message. In our project we use the Hmac-Sha-256 algorithm. Additionally, our cryptographic algorithm scheme includes Nonce value [6] which is used only once. The Nonce value is used as an initializing vector. When we evaluate our project in terms of attacks, we look networks attacks. The main purpose of the network layer in IoT is to provide a secure data transmit between the network?s node. The reason of spoofing attack is that adversary node can get right of entry to the IoT system. IoT systems usually meet the Ip spoofing and RFID spoofing attacks. To prevent these attacks, we need to handle the issue of identification. In our project we use the Nonce value to handle the identification. So we prevent the spoofing attacks. Also the purpose of using Nonce value is to prevent replay attacks on network. Cryptographic Hash Algorithms prevent the side-channel attack, Brute force attack and Collision attack[7]. The proposed cryptographic algorithm scheme includes HMAC/SHA-256 hash function to handle the these attacks. So we have provided integrity of the message with hash function. One of the most important security services in IoT is confidentiality of the transmitted data. We used lightweight symmetric encryption algorithm PRESENT to achieve the confidentiality. We can prevent Man-in-the-middle attack, which is one of the most common attack with using the PRESENT an ultra-lightweight block cipher encryption algorithm[8].

IV. EXPERIMENT

In the implementation we considered the IoT smart home domain. According to the scenario, smart home includes different kinds of several sensors, which are communicating with the gateway through an unreliable transmission media. We aim to ensure secure communication within this local area. We used arduino uno board as an IoT end-device with any type of sensor such that humidity, temperature etc. Arduino has ATmega328p microprocessor [9] embedded on it, which has 2kB SRAM, 32kB flash memory and 2kB EEPROM. Also, DFRobot Ethernet Shield is used to connect to Internet. An Ubuntu 18.04 LTS deployed pc is used as a gateway. Between gateway and IoT end-device UDP protocol is used since it is easy to launch. Top view of the environment configuration is given in Figure4.

In this scenario, firstly, the gateway and arduino node should share a key via Diffie-Helman Key Exchange algorithm. Later, gateway generates a nonce, that is assigned as a symmetric key between node and gateway. Also generated nonce value is utilized in identification. Since, the nonce value is used in both identification and encryption, it is renewed periodically such as in every hour. Afterwards, gateway sends the symmetric

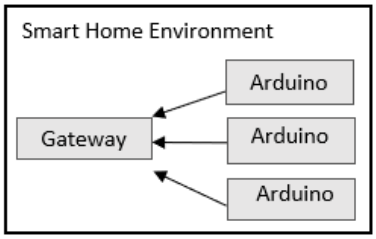

Fig. 4. Configuration of environment

key to the node by encrypting via shared key. After finishing this procedure, the secure communication can start. Step by step explanation of this procedure can be seen in the Figure5.

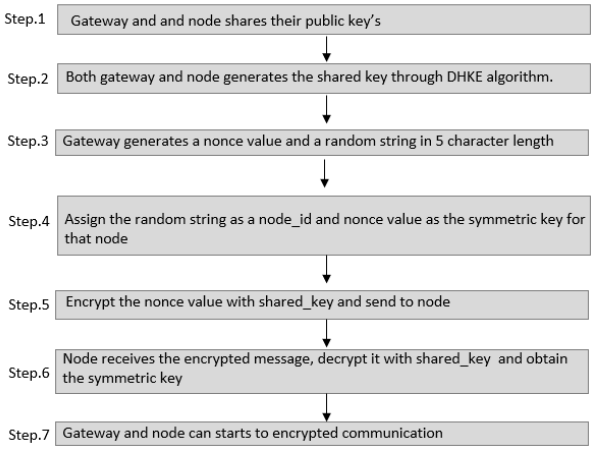

Fig. 5. Step by step explanation of the scenario

V. RELATED WORK AND DISCUSSION

In recent year, the number of limited devices is increasing. So on the literature review we see many study on lightweight cryptographic algorithm . In paper[10], test performance of four different lightweight encryption algorithm. Lightweight encryption algorithms are TEA, KATAN,KLEIN and HIGHT. Authors implemented the study on the Atmel ATtiny45 microcontroller. The study shows memory efficiency, energy consumption in the term of the performance analysis.

In [11], the generic Publish-Subscribe architecture provide privacy for IoT by ABE scheme. There is AES for encrypted messages to ensures ciphertext size. The paper designed secure scheme to provide confidentiality and authentication. The authors uses cryptographic schemes for encryption but this techniques has disadvantage. This scheme is computational overhead for limited end devices.

The other paper [12] proposed a LRBC which is a new lightweight encryption method. This method provide data security on perception layer. LRBS uses Feistel structure as a DES. The structure of LRBS improves for IoT devices.

This article [1] outlines specific vulnerabilities and possible solutions for IoT devices. There are some security issues

in IoT area: First, an Iot application should secure data. Then it should ensure the operation (i.e. sensor operation, data transmission etc.) safety. Finally, it should also handle the information security. This article also explain security challenges for each IoT layer. In our study, we are interested in network layer security, so we examined the challenges and solutions proposed for this layer in this article.

Xin-Wen Wu et al.[13] mentions that all IoT architectures share some common components such as end devices, edge, and platform. Due to their nature, IoT devices should be affordable thus they are limited in size, energy and their capacities of computing and storage. The physical devices may be connected directly to other physical devices, edge platforms, gateways and since the IoT hubs and gateways are usually well-resourced devices one may argue that as long as the gateways are well protected, it may be sufficient to provide minimum security to lightweight devices. But they also argue that this viewpoint is questionable at best. They proposed a new lightweight security protocol as well as a good comparison between known lightweight security protocols. Their protocols use a lightweight symmetric algorithm for encryption. In the paper ensuring security with a one-key-for-one-file approach was argued. The proposed algorithm can replace IPSec suite, to achieve a higher level of security with very low resource consumption.

VI. CONCLUSION AND FUTURE WORK

In our study we proposed a cryptographic scheme which includes confidentiality, integrity and availability on IoT network protocol for provide a secure channel to exchange data transmit. Our cryptographic scheme is suitable for limited end devices. So our proposed scheme is not suitable for every IoT device because of limited device. In future studies, the same cryptographic scheme can be created with the Hummingbird-2 Lightweight Authenticated Encryption algorithm instead of PRESENT, and its efficiency can be tested.

REFERENCES

[1] A. Kamble and S. Bhutad, "Survey on internet of things (iot) security issues & solutions," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, pp. 307–312, IEEE, 2018.

[2] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in *International workshop on cryptographic hardware and embedded systems*, pp. 450–466, Springer, 2007.

[3] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[4] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 international conference on computer science and electronics engineering*, vol. 3, pp. 648–651, IEEE, 2012.

[5] S. Samonas and D. Coss, "The cia strikes back: Redefining confidentiality, integrity and availability in security.," *Journal of Information System Security*, vol. 10, no. 3, 2014.

[6] R. Falk, H.-J. Hof, and U. Meyer, "Method for cryptographically transmitting data between network nodes using a nonce value," July 28 2015. US Patent 9,094,818.

[7] Y. Maleh and A. Ezzati, "A review of security attacks and intrusion detection schemes in wireless sensor networks," *arXiv preprint arXiv:1401.1982*, 2014.

[8] H. Demirci, İ. Taşkın, M. Çoban, and A. Baysal, "Improved meet-in-the-middle attacks on aes," in *International Conference on Cryptology in India*, pp. 144–156, Springer, 2009.

[9] A. Coorporation, *Atmel atmega328p datasheet*, 2011.

[10] V. K. Jha, "Cryptanalysis of lightweight block ciphers," *Aalto University School of Science Degree Programme of Computer Science and Engineering, Master's Thesis*, 2011.

[11] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of attribute-based encryption: Toward data privacy in the iot," in *2014 IEEE International Conference on Communications (ICC)*, pp. 725–730, IEEE, 2014.

[12] A. Biswas, A. Majumdar, S. Nath, A. Dutta, and K. Baishnab, "Lrbc: a lightweight block cipher design for resource constrained iot devices," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–15, 2020.

[13] X.-W. Wu, E.-H. Yang, and J. Wang, "Lightweight security protocols for the internet of things," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–7, IEEE, 2017.